Information Security Policy

EXECUTIVE SUMMARY

Holmes Murphy takes seriously the obligation of protecting the confidentiality, integrity, and availability of the data that has been entrusted to us. We understand and agree that the protection of confidential data is of the most important concern.

To fulfill our commitment to protect confidential data, we have implemented and maintained a comprehensive Information Security Program that aligns with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF).

Based on the criticality of data and guidance from the Centers for Medicare and Medicaid (CMS), which enforces HIPAA standards, Holmes Murphy has deemed the criticality of systems to be at the “moderate” level as defined by FIPS-199.

Commitment

Our commitment to our clients, partners, and employees:

- Treat your data like it is our own.
- Follow all required laws and regulations to protect data and privacy
- Never share your confidential data with any external parties without your expressed consent.

1.0 – Security Training

- The organization acknowledges that employees are the greatest defense in our layered security program. As such, all employees receive information security training upon hire and annually thereafter.
- Ongoing awareness campaigns of current information security threats and trends are provided to keep information security at the top of mind.

Relevant Policies and Procedures

Employee Awareness and Training Policy
Phishing Procedures
Internet Usage and Filtering Policy
Physical Security Policy
Acceptable Use Policy

2.0 – Access Controls

- Minimum necessary standards enforced.
- Role-based access controls are utilized to restrict access to data on a need- to know basis and only by authorized personnel whose job responsibilities require it.
- Technical controls are in place including but not limited to strong password requirements (complexity, rotation, etc.,) and multifactor authentication.

Relevant Policies and Procedures

Identify Access Management Policy
Authentication Standard
BYOD/Mobile Device Policy
Third Party Access Security Policy

3.0 – LOGGING AND MONITORING

- A Security Information & Event Management (SIEM) solution is in place to provide a holistic view of the organization’s network and systems. The SIEM provides 24x7 continuous monitoring, data analysis, threat intelligence, and security incident reporting.

Relevant Policies and Procedures

Security Event Logging Standard
Security Monitoring Policy

4.0 – Vulnerability Scanning and Penetration Testing

- Vulnerability scanning is performed monthly, and any deficiencies are addressed appropriately.
- Penetration testing is performed annually by an external third party.
- Any identified deficiencies are reviewed, and remediation plans developed.

Relevant Policies and Procedures

Vulnerability Management Policy
Incident Response Policy
Incident Response Plan

5.0 – Secure System Configuration and Maintenance

- Baseline configuration is used to deploy new systems with appropriate application and security settings. The organization has a System Maintenance Standard that is followed to identify and keep system and devices patched and up to date.

Relevant Policies and Procedures

Server Security Policy
Virtualization Security Policy
Workstation Security Policy
Database Security Policy
Portable Storage Device Policy
Perimeter Security Policy
Secure SDLC Policy
Project Management Policy
Secure Development Standard
Software Installation Policy
Asset Management Policy
System Patching Standard
Change Management Policy

6.0 – Business Continuity and Disaster Recovery

- In the case of a business interruption or a disaster affecting the organization, the organization is ready to respond quickly and appropriately. A thoroughly vetted and tested Business Continuity and Disaster Recovery Plan is in place to guide the organization and allow the business to provide services as designed.

Relevant Policies and Procedures

IT Disaster Recovery Plan
HMA Disaster Preparedness Plan
Data Backup and Retention Plan

7.0 – Incident Response and Management

- The organization has an Incident Response Plan in place to adequately respond to a security incident. The security team and responsibilities have been documented with its plan and are tested annually to ensure the organization is ready when an incident occurs.

Relevant Policies and Procedures

Incident Response Policy
Incident Response Plan

8.0 – Physical Security

- Physical security controls include video surveillance, alarm systems, electronically controlled doors (badge access), visitor sign in and escort procedures
- Co-located servers are hosted at a SOC2 Type II certified facilities.

Relevant Policies and Procedures

Physical Security Policy
Identity and Access Management Policy
Telework policy
Virtual Private Network Policy

9.0 – Risk Management

- An Information Security Risk Management Program is in place to continually manage risk to the organization from internal and external threats. Identified items are maintained on a risk register. An annual third-party risk assessment is also performed to identify opportunities for improvement.
- The organization has and maintains a robust set of security policies, stands, and procedures based on NIST Special Publication 800-53. These are reviewed and acknowledged by staff annually.
- Vendor Management best practice is used to ensure that privacy and security are maintained by all vendors and partners and that data is treated with the same care and importance as is performed at this organization.
- Critical vendors are put through appropriate due diligence before engaging and annually thereafter to confirm proper controls exist.

Relevant Policies and Procedures

Information Security Council Charter
Risk Management Program
Risk Assessment Policy
System and Service Acquisition Policy
Service Level Agreement Standard
Merger & Acquisition Risk Assessment Standard

10.0 – Encryption

- All Personally Identifiable Information (PII), Protected Health Information (PHI), or similar confidential or restricted data as described in the company's data classification standard is protected with encryption during transmission over public networks.
- All desktop and laptop workstations utilize volume or disk encryption to ensure data at rest cannot be accessed without authorization.

Relevant Policies and Procedures

Encryption and Certificate Management Standard
Portable Storage Device Policy
BYOD/Mobile Device Security Policy
Wireless Network Policy

11.0 – Anti-Malware and Threat Detection/Prevention

- Anti-virus solutions are utilized to recognize and block malware and reduce phishing attacks.
- Intrusions Detection Systems are in place to alert on suspicious activity or policy violations.
- Intrusion Prevention System is in place to examine network traffic and prevent vulnerability exploits.

Relevant Policies and Procedures

Anti-Malware Standard

12.0 – Data Retention and Disposal

- Data is retained and disposed of according to the organization's data retention & destruction standards.

Relevant Policies and Procedures

Data Governance Policy
Portable Storage Device Policy

Data Retention Standard
Data Destruction Standard
Data Recovery Standard
Data Classification Standard

13.0 – Privacy and Compliance

- The privacy policy is supported by the practices included in our information security and risk management policies that have been developed to comply with today's complex world of global data privacy and regulatory compliance.

Relevant Policies and Procedures

Privacy Policy
Data Classification Standard
Data Governance Policy
HIPAA Handling Procedures
Employee Privacy Notification
Web Privacy Notification

14.0 – Network Security

- Utilizes a defense in depth strategy by employing firewalls, routers, architected security zones and continuous monitoring to detect and/or block malicious traffic.
- System availability is achieved by utilizing redundant technologies, regularly scheduled maintenance, and mature change control processes.
- Network devices and appliances are constantly monitored for performance, security and utilize redundant power, UPS, and backup generators.

Relevant Policies and Procedures

Perimeter Security Policy
Encryption and Certificate Management Standard
Security Monitoring Policy
Wireless Network Standard
Virtual Private Network Policy

15.0 – Backup and Retention

- Backup solutions are in place to ensure data is available and consistent with company Business Continuity (BC) and Disaster Recovery (DR) requirements.
- Backups are verified daily.
- Regular test restorations are performed to demonstrate functionality and compliance.
- The record retention policy complies with state and federal retention laws.

Relevant Policies and Procedures

Data Retention Standard
Data Destruction Standard
Data Recovery Standard
Database Security Policy

16.0 – Data Loss Prevention

- Require device whole disk encryption.
- USB device restrictions.
- Network monitoring and alerts for data exfiltration.
- Secure email and File Transfer.
- Mobile Device Management software and authentication PIN required on mobile devices.
- Data destruction procedures for physical and logical devices to secure proper disposal information.
- Data classification policies and procedures.

Relevant Policies and Procedures

Data Governance Policy
Asset Management Policy
BYOD/Mobile Device Security Policy
Software Installation Policy

17.0 – Enforcement and Auditing

17.1 **Policy Enforcement**

Any violations of this policy may result in disciplinary action up to and including termination of employment.

17.2 **Auditing Clean Up**

The Information Security team will ensure that each required test has been completed and any deficiencies addressed as required or document exceptions via the risk management program.

Approved By	Title	Date
André Carroll	Analyst	September 2022
Bryan Thompson	Information Security Officer	October 2023